IFW AF

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 42

Application Number	09/727,147
Filing Date	11/29/2000
First Named Inventor	Halme
Art Unit	2662
Examiner Name	Sefcheck
Attorney Docket Number	KOL-015 (formerly BER-015)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
- [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

Credit Card authorization for appeal brief filing fee of $250 included herewith

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Ronald Craig Fish, A Law Corporation		
Signature	Ronald C. Fish		
Printed name	Ronald C. Fish		
Date	5/20/2005	Reg. No.	28,843

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Ronald C. Fish		
Typed or printed name	Ronald Craig Fish	Date	5/20/2005

PTO/SB/17 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 250

Complete if Known	
Application Number	09/727,147
Filing Date	11/29/2000
First Named Inventor	Halme
Examiner Name	Sefcheck
Group Art Unit	2662
Attorney Docket No.	KOL-015 (formerly BER-015)

METHOD OF PAYMENT

1. ☐ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 06-0932

Deposit Account Name: Ronald Craig Fish, a Law Corporation

☒ Charge Any Additional Fee Required and Credit Any Overpayments Under 37 CFR 1.16 and 1.17

☒ Applicant claims small entity status. See 37 CFR 1.27

2. ☒ **Payment Enclosed:**

☐ Check ☒ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 395.00

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below	Fee Paid
Total Claims	-20** = 0	X	25	= 0
Independent Claims	- 3** = 1	X	100	=
Multiple Dependent			0	= 0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	500	219	250	Notice of Appeal	
120	500	220	250	Filing a brief in support of an appeal	250
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** ($)

SUBMITTED BY

Name (Print/Type)	RONALD CRAIG FISH	Registration No. (Attorney/Agent)	28,843	Telephone	408 866 4777
Signature	Ronald C. Fish			Date	5/20/05

Complete (if applicable)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Halme	Art Unit:	2662
		Examiner:	Sefcheck
Serial No.	09/727,147	Docket No.	KOL-015 (formerly BER-015)
Filed:	11/29/2000		

For: DATATRANSMISSIONCONTROLANDPERFORMANCEMONITORINGMETHODOFAN IPSEC LINK IN A VIRTUAL PRIVATE NETWORK (FORMERLY DATA TRANSMISSION CONTROL METHOD)

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Va. 22313-1450

May 20, 2005

APPLICANT'S APPEAL BRIEF

REAL PARTY IN INTEREST

The real party in interest is Stonesoft OY

RELATEDAPPEALSANDINTERFERENCES

None

STATUS OF CLAIMS

Claims 1-22 are pending. Claims 1-20 are finally rejected and are appealed. Claims 21 and 22 are allowed.

STATUS OF AMENDMENTS

The amendment of 7/13/2004 has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

Generally, the invention is a method and apparatus to monitor the performance of an IPSEC secure protocol tunnel link between computing nodes on each end of the tunnel. IPSEC does not have any native method for monitoring the continued operability or performance level of a tunnel.

The invention provides a way to do this. Special IPSEC acknowledge packets (IPSEC ack packets) are generated and sent after at least a predetermined number of IPSEC packets are received post transmission of the last IPSEC ack packet or upon reception of an IPSEC packet after a timeout has occurred following transmission of the last IPSEC ack packet. In some embodiments, the number of received IPSEC packets and/or the number of received bytes are counted at the destination node and these counter values and a sequence number of the last received IPSEC packet are included in the IPSEC acknowledge packet when they are generated and sent. The sending node stores sending times as timestamps, SPI field contents and sequence numbers of sent IPSEC packets for a period of time to allow the sending node to calculate the round trip time of the IPSEC tunnel. Round trip time can be calculated by noting the reception time of an IPSEC packet with a sequence number of a sent IPSEC packet in it and comparing that reception time to the time of sending of the IPSEC packet which had that sequence number. The packet success rate can also be calculated by calculating the ratio of sent IPSEC packets and received acknowlegments.

Independent claim 1 claims is a method claim which calls for:

employing the IPSEC protocol to tunnel IP packets between the source network node and the destination network node (page 1, lines 23-35, page 4, lines 10-31, page 5 lines 10-15, Figure 3 LAN A, A1, PA1, 10, PB1, B1, LAN B);

transmitting an acknowledgment packet if at least one of a first condition and second condition is fulfilled and defining those conditions (page 6, lines 9-25, Figure 6 steps 610 and 620, page 14, lines 22-32).

Independent claim 2 claims is a method claim which calls for:

employing the IPSEC protocol to tunnel IP packets between the source network node and the destination network node (page 1, lines 23-35, page 4, lines 10-31, page 5 lines 10-15, Figure 3 LAN A, A1, PA1, 10, PB1, B1, LAN B);

transmitting an acknowledgment packet which includes the sequence number of the last received IPSEC packet (page 14, lines 22-24 and lines 28-30, Figure 6, steps 610 and 620) and containing a value indicative of the amount of data received (page 14, lines 28-30, Figure 6, steps 610 and 620) if at least one of a first condition and second condition is fulfilled and defining those conditions (page 6, lines 9-25, Figure 6 steps 610 and 620, page 14, lines 22-32).

Independent claim 8 claims is a method claim which calls for:

employing the IPSEC protocol to tunnel P packets between the source network node and the destination network node (page 1, lines 23-35, page 4, lines 10-31, page 5 lines 10-15, Figure 3 LAN A, A1, PA1, 10, PB1, B1, LAN B);

transmitting an acknowledgment packet if at least one of a first condition and second condition is fulfilled and defining those conditions (page 6, lines 9-25, Figure 6 steps 610 and 620, page 14, lines 22-32);

storing the sequence number and transmission time of each IPSEC packet transmitted from the source network node to the destination network node (page 14, lines 22-24 Figure 6, step 610) and determining the round trip time based upon the stored transmission time and the reception time of the ack packet (page 14, lines 33-35, Figure 6, step 630).

Independent claim 9 is a method claim which calls for monitoring active and inactive communication links between a source network site and a destination network site where the active communication link employs the IPSEC protocol to tunnel IP packets between the source network node and the destination network node (page 1, lines 23-35, page 4, lines 10-31, page 5 lines 10-15, Figure 3 LAN A, A1, PA1, 10, PB1, B1, LAN B), the method for monitoring the active communication link comprising

transmitting an acknowledgment packet if at least one of a first condition and second condition is fulfilled and defining those conditions (page 6, lines 9-25, Figure 6 steps 610 and 620, page 14, lines 22-32);

storing the sequence number and transmission time of each IPSEC packet transmitted from the source network node to the destination network node (page 14, lines 22-24 Figure 6, step 610) and determining the round trip time based upon the stored transmission time and the reception time of the ack packet (page 14, lines 33-35, Figure 6, step 630)

the method for monitoring the inactive communication link comprising (page 8, lines 26-36):

transmitting a probe packet from the source to the destination via the inactive link (page 15, lines 34-36, Fig. 7, step 710, page 19, lines 1-2) and storing its transmit time (page 15, lines 37, page 19, lines 3);

sending a response packet from the destination to the source as a response to

receiving the probe packet (page 16, lines 1-2, Fig. 7, step 720, page 19, lines 4-5);

determining the round trip time of the inactive communication route from the difference between the reception time of the response packet and the transmission time of the probe packet (page 16, lines 3-6, Fig. 7, step 730, page 19, lines 6-8);

maintaining the present status of the active and inactive links or replacing the active link with and inactive link based upon the results of the monitoring (page 5, lines 10-36, page 8, lines 26-36, page 9, lines 18-33, page 12, lines 24-38 and page 13, lines 1-36, page 11, lines 15-19, page 22, lines 24-37, Figures 4 and 5).

Independent claim 11 is directed to a network node programmed to carry out the method of process claim 2 but determining the packet success rate from the information in the ack packet. The process calls for:

a means to implement an IPSEC tunnel between a source and destination to tunnel IPSEC packets to tunnel IP packets therebetween (page 9, lines 1-31, page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1);

means for sending ack packets for the IPSEC packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, line 9 to page 10, line 7, Figure 6, step 620, page 15, lines 15-16, Figure 6, 620);

means for receiving ack packets for IPSEC packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 7, lines 9-12, Figure 6, step 620, 630);

means for obtaining the sequence number of an IPSEC packet from the ack packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 7, lines 9-12; Figure 6, step 620, 630);

means for obtaining from the ack packet a value regarding how much data was recevied via the communication link (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 7, lines 9-12, Figure 6, step 620, 630); and

means for determining the packet success rate (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 16, lines 29-31).

Independent claim 13 is a means plus function apparatus claim defining a network node in the following terms:

means for communicating over an IPSEC communications link with a second network node to tunnel IP packets to the second node (page 21, lines 26-27, Figure 1 A1

and B1, 10, PA1, PB1, page 9, lines 4-16);

means for sending IPSEC packets containing IP packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, line 23);

means for receiving acknowledge packets for IPSEC packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, line 25);

means for obtaining a sequence number of an IPSEC packet from a received ack packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 26-28);

means for storing in a memory means the sequence number and the transmission time of each IPSEC packet transmitted by the network node (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 26-28);

means for determining the round trip time of the communication link on the basis of reception time of an ack packet and the stored transmission time of the corresponding transmitted packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 26-28).

Independent claim 14 is an apparatus claim defining a network node for communicating with a second network node using an IPSEC protocol communication link, stated in the following means plus function terms:

means for communicating over an IPSEC protocol communication link to tunnel IP packets transmitted from the second network node (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16);

means for sending IPSEC packets containing IP packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, line 23);

means for transmitting an ack packet if at least one of a first and second condition is satisfied (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 16, lines 13-15);

said first condition being the reception of at least a predetermined number of IPSEC packets after transmission of the previous ack packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 16, lines 13-15);

said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous ack packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 16, lines 13-15).

Independent claim 15 defines a network node in the following means plus function terms:

means for communicating over a IPSEC protocol communication link with a second network node in order to tunnel IP packets transmitted from the second network node (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16);

means for receiving IPSEC packets containing IP packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 11);

means for transmitting an ack packet if at least one of a first condition and a second condition is fulfilled (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 13-15);

means for inserting a sequence number of a received IPSEC packet and at least one value corresponding to the amount of data received via the communication link in said ack packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 16-18);

said first condition being reception of at least a predetermined number of IPSEC packets after transmission of the previous ack packet and the second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous ack packet (page 16, lines 13-15).

Independent claim 18 is a means plus function network node claim which defines the following network node:

means for communicating over a IPSEC protocol communication link with a second network node in order to tunnel IP packets transmitted from the second network node (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16);

means for transmitting an ack packet if at least one of a first condition and a second condition is fulfilled (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 13-15);

said first condition being reception of at least a predetermined number of IPSEC packets after transmission of the previous ack packet and the second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous ack packet (page 16, lines 13-15)

means for sending IPSEC packets (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, page 16, line 23);

means for receiving acknowledge packets for IPSEC packets transmitted by the network node (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, line 25);

means for obtaining a sequence number of an IPSEC packet from a received ack packet (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 16, lines 26-28);

means for obtaining a value from the ack packet, said value corresponding to the amount of data received via the communication link by the second network node (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 17, lines 22-25);

means for determining the packet success rate of the communication link at least partly on the basis of said value (page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 18, lines 1-5).

Independent claim 19 is a software program product claim for a network node for communicating with the IPSEC protocol with a second network node, comprising:

software program code communicating over an IPSEC protocol communication link with a second network node in order to tunnel IP packets transmitted from the second network node (Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38 to page 22, lines 1-3);

software program code for receiving IPSEC packets containing IP packets (Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38 to page 22, lines 1-3, page 15, lines 15-22);

software program code means for transmitting an ack packet if at least one of a first and a second condition is fulfilled,

said first condition being the reception of at least a predetermined number of IPSEC packets after transmission of the previous ack packet, and

the second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous ack packet (Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38 to page 22, lines 1-3, page 15, lines 15-22)

software program code means for receiving ack packets for IPSEC packets transmitted by the network node (page 22, lines 4-5, Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38, page 15, lines 15-22);

software program code means for obtaining a sequence number of an IPSEC packet from a received ack packet (page 22, lines 6-7, Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38, page 15, lines 15-22);

software program code means for obtaining a value from the ack packet, said value corresponding to the amount of data received via the communication link by the second network node (page 22, lines 8-9, Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38, page 15, lines 15-22);

software program code means for determining the packet success rate of the communication link at least partly on the basis of said value (page 22, lines 11-12, Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38, page 15, lines 15-22).

Independent claim 20 is a software program product for a network node which controls the network node to communicate with the IPSEC protocol with a second network node via a communication link comprising:

software program code communicating over an IPSEC protocol communication link with a second network node in order to tunnel IP packets transmitted to said second network node (Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38 to page 22, lines 1-3, page 21, lines 26-28);

software program code sending IPSEC packets containing IP packets (Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38 to page 22, lines 1-3, page 15, lines 15-22, page 21, lines 26-28);

software program code receiving ack packets for said IPSEC packets (page 22, lines 4-5, Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38, page 15, lines 15-22, page 21, lines 26-28);

software program code obtaining a sequence number of an IPSEC packet from a received ack packet (page 22, lines 6-7, Figure 6, Figure 1 A1 and B1, 10, PA1, PB1, page 9, lines 4-16, page 21, lines 36-38, page 15, lines 15-22, page 21, lines 26-28);

software program code storing in a memory means the sequence number and the transmission time of each IPSEC packet transmitted by the network node via the communication link (page 14, lines 22-24 Figure 6, step 610, page 21, lines 26-28);

software program code determining the round trip time of the communication link on the basis of the reception time of an acknowledgment packe and the stored transmission time of the

corresponding transmitted packet (page 14, lines 33-35 Figure 6, step 610, page 21, lines 26-28)

GROUNDS OF REJECTIONS TO BE REVIEWED ON APPEAL

Claims 1-8 and 11-20 were rejected under 35 USC 103(a) as obvious over Jorgensen (US 6,680,922) and Chiu et al. (US 6,526,022). Claims 9-10 are rejected under 35 USC 103(a) as obvious over Jorgensen (US 6,680,922) and Chiu et al. (US 6,526,022) and further in view of Tam (US6,622,172) and Garcia-Luna-Aceves et al. (US 20010013856A1).

ARGUMENT

Obviousness Rejection of Claims 1-8

Claims 1-8 were rejected under 35 USC 103(a) as obvious over Jorgensen (US 6,680,922) and Chiu et al. (US 6,526,022). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching, suggestion or incentive to do so. In re Bond, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). Suggestion arises from one of ordinary skill in the art perceiving a liklihood of success in solving the problem the inventors solved by making the combination. In other words, the consistent criterion for determination of obviousness is whether the prior art would have suggested to one of ordinary skill in the art that this process should be carried out *and would have a reasonable likelihood of success, viewed in the light of the prior art.* See Burlington Industries v. Quigg, 822 F.2d 1581, 1583, 3 USPQ2d 1436, 1438 (Fed.Cir.1987); In re Hedges, 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed.Cir.1986).

Here, the problem the inventors solved was how to monitor and measure the performance of an IPSEC private tunnel communication link when neither the IPSEC protocol nor the TCP/IP protocol provides a way to monitor and measure the performance of an IPSEC tunnel. This is a useful feature because often multiple private tunnel data paths taking different routes through different gateways, different ISPs and different legs and routers on the internet are available to send data from a first node to a second node.

This problem is basically solved by sending special IPSEC acknowledgment packets back from the destination node to the source node in response to receipt of an IPSEC packet from the source node if either one of two conditions are satisfied. Each IPSEC acknowledgment packet contains the sequence number of the IPSEC packet just received and may contain a counter value indicative of the amount of data received in some embodiments. These ack packets are not the ack packets generated in the TCP/IP protocol and they have a special data structure in that

they contain at least the sequence number of the IPSEC packet received just before the IPSEC acknowledgment packet was sent. Specification, page 6, lines 9-17.

The two conditions under which an IPSEC acknowledgment packet will be sent are: 1) an IPSEC acknowledgment packet will be sent every Nth IPSEC packet received (Specification, page 6, lines 11-13); and 2) reception of an IPSec packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet (Specification, page 6, lines 18-23).

Claim 1 Distinction Over The Prior Art

The transmission of these IPSEC acknowledgment packets is recited in claim 1 in the following language:

> - transmitting an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled, said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and said second condition being the reception of an IPSec packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

The claim limitation "transmitting an acknowledgment packet" should be interpreted as requiring generation of an IPSEC packet containing at least the sequence number of the IPSEC packet received to which the transmission of the acknowledgement packet is a response. A limitation in a claim should be interpreted in accordance with the specification and prosecution history, and to do so is not reading limitations into the claim. Under a recent *in banc* decision of the Federal Circuit, claim construction is a job for the judge as it is a question of law. Markman v. Westview Instruments, Inc., 52 F.2d 967 (Fed. Cir. 1995). Three intrinsic sources of data on this subject are the specification, the language of the claims themselves and the prosecution history. The judge is free to consider extrinsic sources also such as expert testimony, dictionaries, prior art references etc., but in the recent Vitronics decision, the Federal Circuit held that the meaning of the claims is almost always ascertainable from the intrinsic evidence and resort to extrinsic evidence is the exception rather than the rule. Vitronics Corp. v. Conceptronic Inc., 39 USPQ2d 1573 (Fed. Cir. 1996). Further, Vitronics holds that it is legal error to rely on extrinsic evidence where the meaning of the claims is clear from the intrinsic evidence.

It is always necessary to review the specification to determine whether the inventor has used any terms in a manner inconsistent with their ordinary meaning. The specification acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication. The specification contains a written description of the invention which must be clear

and complete enough to enable those of ordinary skill in the art to make and use the invention. Thus, the specification is always relevant to the claim construction analysis. Usually it is dispositive; it is the single best guide to the meaning of a disputed term. Vitronics Corp. v. Conceptronic Inc., 39 USPQ2d 1573, 1577 (Fed. Cir. 1996). If the specification does not give a term a unique or special meaning, the term will be given its ordinary meaning to one of skill in the art. Ekchian v. Home Depot Inc., 104 F.3d 1299, 41 USQP2d 1364 (Fed. Cir. 1997). The Federal Circuit has held that a patentee is bound by the specification in interpreting his claims even when the specification requires a narrower interpretation of the claims than the patentee desires. Fonar Corp. v. Johnson & Johnson, 821 F.2d 627, 3 USPQ2d 1109 (Fed. Cir. 1987). A narrower definition derived from the specification and prosecution history will prevail over a broader dictionary definition. Texas Instruments Corp. v. Cypress Semiconductor Corp, 90 F.3d 1558, 39 USPQ2d 1492 (Fed. Cir. 1996); Greiner v. Mari-Med, 962 F.2d 1031, 22 USPQ2d 1526 (Fed. Cir. 1992). Further, where a meaning for a claim term gleaned from the only embodiment taught in the specification is narrower and more specific than the general dictionary definitions of the words used in the claim, the meaning gleaned from the specification controls. Toro Co. v. White Consolidated Industries, Inc., 53 USPQ2d 1065, 1069 (Fed. Cir. 1999).

Here, the term acknowledgment packet is broad and reads on both IPSEC acknowledgment packets and TCP/IP acknowledgment packets. However, the TCP/IP acknowledgment packet meaning makes no sense since TCP/IP acknowledgment packets require as part of their content a sequence number which is in the header of the TCP/IP packet, and this header is encrypted along with the rest of the TCP/IP packet in the payload section of the IPSEC private tunnel packet. To send a TCP/IP acknowledgement packet from the tunnel gateway upon receipt of an IPSEC packet would be impractical because the payload section of the IPSEC packet would have to be decrypted. Therefore, the only interpretation that makes sense is the IPSEC packet interpretation and the possible other interpretation lends enough indefiniteness to the claim to invite interpretation in light of the specification. Where the claim terms chosen are not defined in the claim and are of such a broad nature as to render the meaning of the claim indefinite, such claim terms invite resort to the specification to clarify their meaning. Johnson Worldwide Associates Inc. v. Zebco Corp., 50 USPQ2d 1607, 1610 (Fed. Cir. 1999). However, where the meaning of claim terminology is "sufficiently clear" in the patent specification, that meaning will prevail over a broader dictionary definition. This is so even where the patentee presented a broader dictionary definition to the Patent Examiner during the prosecution in an attempt to broaden a claim. Multiform Dessicants Inc. v. Medzam Ltd., 45 USPQ2d 1429 (Fed. Cir.

1998).

Here, the specification clearly indicates that the acknowledgement packet which is sent is an IPSEC acknowledgment packet which contains the sequence number of the IPSEC packet just received. Thus, this is the correct interpretation of the claim term acknowledgement packet in claim 1 and all claims in issue which contain this same term.

The prior art combination does not contain a teaching of generating special IPSEC acknowledgment packets which contain the sequence number of the IPSEC packet just received and sending it back from the destination node to the source node if either of the two conditions are satisfied. Specifically, Jorgensen teaches a virtual private network using a wireless PTMP transmission system which uses IPSEC as a method of security encryption. Jorgensen does teach using IPSEC protocol to tunnel IP packets on a communication link between a source network node and a destination network node. But the Examiner admits that Jorgensen does not teach monitoring the IPSEC protocol link in a manner as claimed in the present invention. The Examiner then asserts that it would have been obvious to modify the teachings of Jorgensen using the teachings of Chiu to achieve the claimed invention.

Jorgensen does not teach the generation and sending of IPSEC acknowledgment packets which contain the sequence number of the IPSEC packet just received.

Therefore, one way for the Examiner's position to be correct, would be if Chiu taught the generation of special IPSEC acknowledgment packets each of which contains the sequence number of the IPSEC packet just received. Chiu would also have to teach sending those IPSEC acknowledgment packets back from the destination node to the source node under one of the two conditions recited in claim 1 and would have to suggest this as a way to monitor the performance of an IPSEC tunnel.

Chiu does not teach generation of special IPSEC acknowledgment packets each of which contains the sequence number of the IPSEC packet just received and sending those IPSEC acknowledgment packets back from the destination node to the source node under one of the two conditions recited in claim 1.

Chiu is addressed to the problem of how to make a TCP/IP multicast reliable without flooding the sending node with TCP/IP ACK and NACK packets from all the numerous destination nodes in the multicast. Chiu solves this problem by teaching a heirarchical structure comprised of a source node and a plurality of "repair heads" each of which talks to a plurality of destination nodes or member stations in the multicast. Chiu teaches use of the ACK windows and assignment of specific ACK windows to specific member stations (destinations) for timing of

transmissions of the ACK messages to spread out the transmission of ACK and NACK messages and avoid flooding. Specifically, Chiu teaches at Col. 7, lines 11 - 37:

> The invention avoids an ACK implosion by spreading out the ACK (and NACK) messages so that a flood of them do not reach the repair head simultaneously. The use by members of the ACK window for timing of transmission of the ACK messages helps to prevent too many ACK messages from reaching the transmitting station at the same time. The ACK messages contain both acknowledgment information for packets received by the member station, and contain NACK information for packets not received by the member station, as based on the sequence numbers of the packets. The term "ACK message" will be used throughout this patent to indicate a message returned by a receiving station to a transmitting station, where the message carries both ACK and NACK information.
>
> The ACK window is defined for a multicast session by establishing the number packets which make a full sequence of ACK windows. Receipt of a full window of packets is an event which triggers transmission of an ACK message by a member station. In a preferred embodiment of the invention, the ACK window size is configurable, and the default number of packets which make a full sequence of ACK windows is thirty two (32) packets.
>
> To prevent many member stations from sending ACK messages at the same time, ACK messages are distributed over the next ACK window. Each member is assigned a window (for example between 1 and 32) for sending its ACK messages.

The ACK and NACK packets Chiu is talking about are TCP/IP ACK and NACK packets. Specifically, at Col. 4, lines 17-67 to Col. 5, line 25 Chiu teaches:

> The TCP portion of TCP/IP (The Connection Protocol) is a layer 4 protocol and establishes reliable communication between the end stations by causing retransmission of packets using the IP protocol.
>
> In a commonly used terminology, the words "datagram" and "message" are often used interchangeably. In an alternative usage, a "message" may be broken into one or more "datagrams". However, in this document the words "datagram" and "message" and "packet" are used interchangeably. A "frame" is used as the messaging unit transferred by the physical layer on a hop between two computers.
>
> Unreliable multicast communication is relatively simple to implement, as the source station simply transmits the datagrams with an address that the designated computers can recognize as a multicast address, and which routers forward. The destination stations then receive any datagrams which they detect. No attempt is made to either identify or retransmit lost datagrams.
>
> Reliable multicast is more difficult to implement. For example, in the case of a few destination computers, the source station must maintain a record of the ACK messages received from each intended destination station so that a datagram missing from any one of the destination stations can be retransmitted. However in the case where there are tens of thousands, even millions, of intended destination stations, the large number of ACK messages will flood the source station and will flood the network. The detrimental effect of too many ACK and too many NACK messages is referred to as ACK implosion or NACK implosion. Administration problems also arise, where for example, a source station has a particular destination station on its list of intended destination stations, and

for some reason that destination station is no longer operational. The source station may then continue indefinetly retransmitting messages while waiting for an ACK from the missing station.

One solution to the reliable multicast problem, where the multicast message is to be received by a group of destination computers, has been to have an administrator (a person or a computer program operated by the person) set up a repair tree. In a repair tree, certain computers are designated as a "repair head". The rest of the computers of the group of destination computers are assigned to a designated repair head. Typically, a source station transmits a multicast datagram onto the network. The datagram should be received by all members of the destination group. Since the datagrams carry a sequence number, each destination station determine if it has missed a datagram. Each station sends an ACK to its repair head upon successful reception of a window of datagrams, and sends a NACK to its repair head upon determining that it has missed a datagram. Upon receipt of an ACK from every member of its repair group, the repair head flushes the datagram from its cache. The repair head retransmits any datagram for which it receives a NACK, until all members of its repair group respond with an ACK for each datagram.

In the event that a repair head is missing a datagram, it NACKs to the source station, and the source station retransmits the datagram. The source station maintains a cache of transmitted datagrams and flushes them after receipt of an ACK from each of the repair heads affiliated with the original source station.

Congestion on the network can result from large numbers of ACK and NACK messages. Particularly, a destination station which is slower than the transmitting source station will miss many multicast datagrams. The resulting NACK messages can cause a NACK implosion and contribute to network congestion. Upon receipt of a NACK message, a source station or repair head will begin retransmission of datagrams, thereby contributing to even more congestion. Congestion can particularly increase when a low bandwidth link is responsible for a number of destination stations being slower than the source station. Each destination station will miss numerous datagrams, and will flood the network with NACK messages, followed by more retransmissions in a feedback cycle which increases congestion.

The Examiner stated it would be obvious to modify the network teachings of Jorgensen by using the method of monitoring a link through the transmission of ACK packets as disclosed in Chiu. In the Examiner's rejection, it is apparent he is relying upon the Chiu teaching of TCP/IP ACK and NACK packets as a teaching of the IPSEC acknowledgment packets of properly interpreted claim 1. It is evident that the Examiner has misinterpreted the claim language of claim 1 apparently thinking that claim 1 calls for the transmission of TCP/IP ACK packets when it actually calls for transmission of IPSEC ACK packets.

The prior art is missing a critical piece of knowledge needed to solve the problem the invention solved. Chiu is silent on the generation of special IPSEC acknowledgement packets which contain the sequence number of the IPSEC packet just received. This is a key claim feature required to solve the problem the inventors solved, and it is completely missing from the

prior art combination.

Where the prior art of a combination of references cited in support of an obviousness rejection does not teach an element needed to solve the problem the claimed invention solved, the obviousness argument must fail. In re Hayes Microcomputer Products, Inc., 982 F.2d 1527, 1541, 25 USPQ2d 1241 (Fed. Cir. 1992) [failure of prior art to teach a claimed method of detecting escape sequences in modems doomed obviousness invalidity argument of infringer even though escape sequences themselves were admittedly in the prior art]. There is no suggestion to support an obviousness rejection based upon a combination of references where the combination of references does not contain all the knowledge needed to make the claimed invention.

There are practical difficulties in modifying Jorgensen with the teachings of Chiu which negate suggestion to make the modification and undercut the viability of the obviousness rejection. As mentioned above in the section on the proper interpretation of "acknowledgment packet", TCP/IP acknowledgment packets require as part of their content a sequence number which is in the header of the TCP/IP packet, and this header is encrypted along with the rest of the TCP/IP packet in the payload section of the IPSEC private tunnel packet. To send a TCP/IP acknowledgement packet from the tunnel gateway upon receipt of an IPSEC packet would be impractical because the payload section of the IPSEC packet would have to first be decrypted and the sequence number in the TCP/IP packet obtained and put in a TCP/IP ACK packet. The TCP/IP packet which would then have to re-encrypted and encapsulated in an IPSEC packet and sent back to the source. There the encapsulated TCP/IP packet would have to be decrypted and the sequence number recovered. Chiu does not teach storing transmission times of the TCP/IP packets to which the TCP/IP ACK and NACK packets are a response. Therefore, calculation of round trip time would not be possible as a form of monitoring. One skilled in the art would reject this approach as too awkward, too slow and lacking in the ability to calculate round trip time which is an important thing to know in monitoring an IPSEC tunnel, especially where several different possible IPSEC tunnels exist and the fastest one is a fact of interest. The Federal Circuit in In Re Newell, 891 F.2d 899, 13 UAPQ2d 1248 (Fed. Cir. 1989) reversed an obviousness rejection upheld by the Board stating:

> "The motivation to make a specific structure is not abstract, but practical, and is always related to the properties or uses one skilled in the art wold expect the structure to have if made."

891 F.2d at 901, 13 UAPQ2d at 1250

Here, the practical difficulties of trying to use TCP/IP ACK and NACK packets between endpoints of a secure IPSEC tunnel which is sending IPSEC packets encapsulating packets of another protocol such as TCP/IP would discourage one of skill in the art from attempting to make the combination proposed by the Examiner. If the combination or modification suggested by the Examiner were to be made, it either would not work at all or would not work well. This is the antithesis of suggestion. It is teaching away from the combination.

A reference may be said to teach away from a proposed combination in support of an obviousness rejection when a person of ordinary skill in the art, upon reading the reference, would be led in a direction divergent from the path that was taken by the applicant to solve the problem the claimed invention solved or would be discouraged from using the teachings of the reference in attempting to solve the problem the claimed invention solved. In re Gurley, 27 F.3d 551, 553, 31 USPQ2d 1130, 1131 (Fed. Cir. 1994). In general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant. 27 F.3d at 533, 31 USPQ2d at 1131. References taken in combination teach away when they would produce a "seemingly inoperative device". 27 F.3d at 553, 31 USPQ2d at 1131-1132. In re Caldwell, 319 F.2d 254, 256, 138 USPQ 243, 245 (CCPA1963) (reference teaches away if it leaves the impression that the product would not have the property sought by the applicant).

Here, an attempt to use the teachings of Chiu in using TCP/P ACK and NACK packets to modify Jorgensen to monitor the performance of the IPSEC tunnel of Jorgensen would seem to yield an inoperative device and method or at least a device and method which would not have the properties sought by the applicant. Support for this argument can be found in the Chiu reference itself at Col. 35, lines 11-52. There, addressing the issue of security, Chiu mentions that sender authentication in a TCP/P mutlicast can possibly be solved using IPSEC protocol or digital signatures in the data messages generated by the sender. However, Chiu teaches that his TRAM protocol is not compatible with any of the security possibilities he mentions and that a security layer must be implemented above the TRAM protocol layer. This means that the TRAM protocol cannot be used with IPSEC tunnels, and this teaches away from combining the TRAM protocol teachings with the Jorgensen IPSEC tunnels.

In other words, the combination of Chiu and Jorgensen would be inoperative. This is because the key to solving the problem is in sending IPSEC ack packets which contain the sequence number of the IPSEC packet just received at the destination node. Chiu teaches using TCP/P ACK and NACK packets to make TCP/P multicast reliable. Even if P packets are tunnelled

in the IPSEC tunnel, the TCP/IP packets are encrypted so the sequence numbers of the received TCP/IP packets are not available to the endpoint nodes of the IPSEC tunnel. The only way the Chiu protocol would work would be behind the IPSEC tunnel endpoints where the IP packets have been recovered and their sequence numbers are available for retrieval and putting in TCP/IP ack packets. But these are not the sequence number of IPSEC packets so the throughput and round trip times of the IPSEC tunnel itself could not be determined using the Chiu ACK and NACK packets. The throughput of the IPSEC tunnel is the number of IPSEC packets received per unit of time. The round trip time is the time from transmission of an IPSEC packet from a source and the time of reception by said source of the IPSEC ack packet sent in response to receipt of the IPSEC packet transmitted by the source. The Chiu TRAM protocol, even if combined with the Jorgensen IPSEC tunnel, would not provide enough information to determine either the round trip time or the throughput of the IPSEC tunnel itself.

The Jorgensen-Chiu combination would also not have the properties sought by the applicant because Chiu does not teach sending an acknowledgement packet if either of the two conditions recited in claim 1 are true. Therefore, even if the combination of Chiu and Jorgensen could be made and there is no technological incompatibility, the claimed combination still would not perform the same functions as recited in claim 1, *i.e., sending an acknowledgement packet if either a predetermined number of IPSEC packets have been received or if an IPSEC packet has been received after a predetermined time has elapsed from transmission* of the last acknowledgement packet.

Chiu is also directed to a different problem than the claimed invention and does not recognize the problem sought to be solved by the applicants. Specifically, Chiu teaches that the TCP flow control mechanism of ACK and NACK packets should be used to make TCP/IP multicasts reliable. He does not recognize that there is no flow control in IPSEC tunnels, and one skilled in the art reading Chiu would perceive no need for additional flow control since the Chiu TRAM protocol already teaches flow control so one skilled in the art would ask himself or herself why would any additional flow control be necessary. Even if the need for flow control in an IPSEC tunnel were perceived, one skilled in the art would reject the TRAM protocol as a way of doing it because Chiu teaches in Col. 35 that his protocol is not compatible with IPSEC. One skilled in the art would believe this since Chiu depends upon TCP ACK and NACK packets which include sequence number of the TCP/IP packets. These sequence numbers are not available at the IPSEC tunnel protocol level because the encapsulated TCP/IP packet is encrypted.

This raises a further reason why one skilled in the art would reject the notion of

combining Chiu with Jorgensen. Chiu teaches the need for and a mechanism to reduce overhead signalling on the network while still making multicast reliable by using repair heads. To use Chiu's TCP ACK and NACK packets inside an IPSEC tunnel would require either additional signalling to send the TCP/IP packet sequence numbers in the clear so that could be incorporated into the TCP ACK and NACK packets, or additional processing to decrypt the encapsulated TCP/IP packets in the received IPSEC packets would be required. Chiu teaches simplifying and reducing overhead signalling, not increasing complexity or increasing overhead signalling.

So Chiu provides a different solution (use of repair heads in a tree structure and scheduling of TCP/IP ACK and NACK packets to avoid flooding) than is required to solve the problem of the invention. The environment in which the invention operates is an IPSEC tunnel which has two endpoints. This is not the multicast environment of Chiu and there are no hierarchically structured repair heads which receive scheduled TCP/IP ACK and NACK packets so as to retransmit missing packets so as to make the multicast reliable without flooding the sender with TCP/IP ACK and NACK packets.

If the applied prior art does not indicate any awareness of the problem solved by the applicants, it is hardly fair to take the position the Examiner has taken that one skilled in the art would perceive suggestion to use the teachings of the reference to solve the problem solved by the claimed invention. In re Nomiya, 509 F.2d 567, 184 USPQ 607 (CCPA 1975). There must, however, be a reason apparent at the time the invention was made to the person of ordinary skill in the art for applying the teaching at hand [to solve the problem the applicants have solved], *or the use of the teaching as evidence of obviousness will entail prohibited hindsight.* Graham v. John Deere Co., 383 U.S. 1, 36, 86 S.Ct. 684, 15 L.Ed.2d 545 (1966). Invention can lie in the discovery of the source of the problem even with the solution is simple once the source of the problem is discovered. In re Nomiya, 509 F.2d at 571.

In Nomiya, the problem solved by the invention was discharge of data of memory cells of a memory circuit with very low capacitance when an IGFET switching transistor with a protective diode is used to store the data or to input signals. The protective diode formed in the same substrate as the IGFET prevent breakdown of the thin oxide gate insulation layer when charge buildup on the gate occurs. The protective diode of the prior art prevented a sufficiently high voltage buildup on the gate to cause punch through of the gate oxide. Unfortunately, it also created a small parasistic bipolar transistor formed between the protective diode and the drain of the IGFET when the protective diode was forward biased by a noise signal. This caused a spontaneous drainage of the stored charge out through the drain region and destroyed the

operation of the memory cell. The solution to this problem was formation of a second protective diode outside the substrate.

The cited prior art in support of the obviousness rejection taught a protective diode in an improved IGFET **but did not recognize that the protective diode could lead to parasitic transistor action that could destroy proper operation of the cell.**

The CCPA held that the failure of the prior art to recognize the problem realized by the inventors was fatal to the obviousness rejection because the obviousness rejection was based upon hindsight reconstruction using the teachings of the applicant to view the prior art. The CCPA noted that there would have been no suggestion in the prior art teaching of a protective diode to add a second protective diode which is outside the substrate. This is because the second diode would be deemed to be superfluous since a first protective diode already existed and the prior art, not recognizing the source of the problem, would not recognize the need for a second protective diode formed outside the substrate in which the IGFET was formed. In Judge Rich's inimitable and clear fashion, the CCPA held:

> "If, as appellants claim, there is no evidence of record that a person of ordinary skill in the art at the time of appellants' invention would have expected the problem in the IGFET to exist at all, it is not proper to conclude that the invention which solves this problem, which is claimed as an improvement of the prior art device... would have been obvious to that hypothetical person of ordinary skill in the art."

509 F.2d at 572, 184 USPQ2d at 613.

Here, neither Jorgensen nor Chiu recognize the need for monitoring the performance of an IPSEC tunnel. Chiu is concerned with making an IP Multicast transport mechanism reliable without flooding the sender with TCP/IP ACK and NACK packets. The TCP/IP ACK and NACK packets are used only by the repair heads to figure out which packets need to be resent to various destinations. This is taught in Chiu at Col 17, lines 21-42 where Chiu teaches the TCP ACK and NACK packets contain the TCP/IP packet sequence number of the first missing TCP packet so that this packet can be resent. That is not the same as sending in an IPSEC ack packet the sequence number of the last IPSEC packet received so that the sender can use the sending time of that IPSEC packet (as identified by the sequence number in the IPSEC ack packet) and the reception time of the IPSEC ack packet sent in response to reception thereof to calculate round trip time through the IPSEC tunnel.

IPSEC packet sending times are not stored in Chiu (nor are TCP/IP packet sending times) so round trip time cannot be calculated in Chiu and there is no mention of the two conditions for sending an IPSEC ack packet recited in claim 1. That is why the teachings of Chiu regarding

sequence number and the lack of teaching of storing sending times would suggest to one skilled in the art that Chiu's TRAM protocol cannot be used to calculate round trip times in an IPSEC tunnel to monitor its performance. Since neither Jorgensen nor Chiu recognize a need to monitor IPSEC tunnel performance, neither suggest combination with the other to solve this problem.

Finally, even if the combination could be accomplished technically, which appears to not be the case, the combination would still fall short of the solution the applicants have provided since there is no teaching of IPSEC ack packets with the sequence numbers of the IPSEC received packets in them or the two conditions under which the IPSEC ack packets are sent. The Examiner recited Col. 16, lines 63-67 as teaching the first condition. This is a misreading of Chiu since that section teaches a TCP ack window and sending a TCP ACK packet after one TCP window of packets has been received. This is not the same as counting the number of IPSEC packets received since transmission of the last IPSEC ack packet and the jump from TCP ACK windows to counting IPSEC packets results from the use of hindsight reconstruction since Chiu teaches his protocol is not compatible with IPSEC.

The Examiner refers to Chiu Col. 17, lines 7-15 as teaching the second condition. This section is also different from condition two because it teaches a straight timeout from sending the last ACK packet. This relates to a condition where the sender has paused. Condition number two is sending of an IPSEC ack packet after a timeout from the sending of the last IPSEC ack packet has occurred and a new IPSEC packet is received. This means the sender has not paused and the IPSEC tunnel is still working. This is a different factual situation from that taught in Chiu.

Independent claim 2

Independent claim 2 contains the following limitations that distinguishes it over the combination of Jorgensen and Chiu:

> *transmitting an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,, wherein said acknowledgement packet comprises at least the sequence number of the last received IPSec packet* **and at least one value corresponding to the amount of data received via the IPSec communication link,**
> said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and
> said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

The italicized limitation should be interpreted the same way as the corresponding limitation

in claim 1. The argument for non obviousness given above for claim 1 is hereby incorporated by reference.

The limitation set off in bold is another element of knowledge that is not present in the combination of Chiu and Jorgensen. Chiu teaches the content of the TC/IP ACK messages he uses at Col. 7, lines 16-20 as containing both acknowledgment information for packets received by member stations and NACK information for packets not received by the member stations, as based upon the seqence numbers of the packets. Chiu also teaches inclusion of a bit map in the TCP acknowledgement packet, but this bit map is not for purposes of calculating how much data was received. Instead, it is included to calculate how much data needs to be resent starting from the sequence number of the first missing TCP packet. The Examiner's citation of Chiu, Col. 36, lines 35-55 and Col. 38, lines 1-7 as teaching sending calculation of the amount of data sent is a misreading to the content of the reference. That passage teaches calculation of the average rate of transmission not the absolute amount of data transmitted.

Therefore, there is no teaching of an ACK packet in Chiu which contains a "value corresponding to the amount of data received via the IPSEC communication link". Since Chiu is not concerned with measuring the throughput of the channel, there is no need in the ACK packets of Chiu to contain a number indicative of the amount of data received via the channel. Chiu is only concerned about which packets were not received. Since Chiu does not recognize the problem of measuring the throughput of an IPSEC tunnel, his ACK packets do not suggest a solution since they do not contain the information needed to solve this problem.

Independent Claim 8

Independent claim 8 contains the following limitation which distinguishes it over the combination of Jorgensen and Chiu:

> - transmitting an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,
>
> said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and said second condition being the reception of an IPSec packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet;

The argument given above for the non obviousness of claim 1 is hereby incorporated by reference based upon interpretation of this sending of an acknowledgement packet limitation from claim 8 in the same way as a corresponding limitation in claim 1.

Claim 8 also contains the following limitations which also are not taught in Chiu or

Jorgensen:

- storing of the sequence number and the transmission time of each IPSec packet transmitted from the source network node to the destination network node in a memory means, and
- determining the round trip time of the communication link on the basis of the reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

In the Chiu TRAM protocol, the sequence number and transmission time of each TCP/IP packet is not stored so there is no suggestion to do this for IPSEC packets. This is fair to say since the problem of monitoring the round trip time of the Chiu multicast data paths is not recognized by Chiu. Chiu teaches at Col. 5, lines 61-67 that the sender of a multicast messages sends numbered datagrams to the repair head which stores them and sends back an ACK message. The sender saves the sent messages (but not the transmission times) until ACK messages are received and then flushes the sent messages from its cache. The same mechanism applies in Chiu to transmissions from the repair head to the destination machines (Col. 6, lines 8-27): the repair head stores the numbered datagrams it sends, but not the transmission times, until it receives ACK messages. Any missing datagrams a destination node did not get are resent until all datagrams have reached all destinations, and then the repair head cache of datagrams is flushed. Also, Chiu does not teach the repair heads storing the reception time of the ACK messages. This is necessary to calculate round trip time. Because Chiu does not store transmission times of the sent IPSEC packet nor reception times at the sender of reception of IPSEC ack packets, round trip times cannot be calculated, and this important element needed for the invention of claim 8 is completely missing from the prior art combination applied against claim 8.

Therefore, Chiu also does not suggest any mechanism or protocol to measure the round trip time of an IPSEC link since he does not even suggest this as either necessary or desirable in a TCP/IP link.

Independent Claim 11 Argument

Claim 11 contains the following limitations which distinguish it over the prior art combination of Jorgensen and Chiu:

- means for sending acknowledgment packets for said IPSec packets containing IP packets,

- means for receiving said acknowledgement packets for said IPSec packets,
- means for obtaining a sequence number of an IPSec packet from said a received acknowledgement packet,
- means for obtaining a value from said the acknowledgement packet, said value corresponding to the amount of data received via the communication link by said second network node, and
- means for determining the packet success rate of the communication link at least partly on the basis of said value.

The limitation:

- means for sending acknowledgment packets for said IPSec packets containing P packets,

is a means plus function limitation, and should be interpreted in accordance with 35 USC 112, Para. 6 to read on the apparatus recited in the specification to carry out the recited function of sending an ack packet for IPSEC packets containing an P packet. Interpretation of means-plus-function claims is controlled by statute 35 U.S.C. 112, Para. 6. That statute states:

> "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."

Therefore, this limitation should be interpreted as requiring a computer programmed to carry out the function of sending an IPSEC acknowledgement packet under either one of the two conditions recited in the specification at page 20, lines 20-25 in response to receipt of an IPSEC packet containing a sequence number, said IPSEC acknowledgement packet containing the sequence number of the IPSEC packet just received and a value corresponding to the amount of data received. (specification page 20, lines 20-25 and lines 30-34, Figure 8, items 821, 822, 862, 874, 860, 870, page 21, lines 26-27, Figure 1 A1 and B1, 10, PA1, PB1, page 9, line 9 to page 10, line 7, Figure 6, step 620, page 15, lines 15-16, Figure 6, 620).

Since this limitation is the hardware superset equivalent of the method step of claim 1 of sending an IPSEC ack packet under one of two conditions, all the same arguments recited above for non obviousness of claim 1 based upon this limitation are applicable here and are hereby incorporated by reference.

Claim 11 also contains the following additional limitations that are not found in the prior art combination:

- means for receiving said acknowledgement packets for said IPSec packets,

- means for obtaining a sequence number of an IPSec packet from said a received acknowledgement packet,

- means for obtaining a value from said the acknowledgement packet, said value corresponding to the amount of data received via the communication link by said second network node, and

- means for determining the packet success rate of the communication link at least partly on the basis of said value.

Chiu does not teach receiving IPSEC acknowledgement packets sent in response to reception of IPSEC packets and extracting both a sequence number of the IPSEC packet to which the ACK packet is a response as well as a value indicative of the amount of data received at the destination node. Chiu's TCP/IP ACK and NACK packets do contain sequence numbers of TCP/IP packets received so that the repair heads can figure out which packets were not received and re-send them to make the multicast reliable. However, there is no value in the TCP/IP ACK and NACK packets which is indicative of the amount of data received by the destination node since that is not part of the Chiu solution. Chiu does not recognize the need for determining the amount of data received, only the need for determining which exact data packets were received. In short, Chiu is not concerned with measuring packet success rate so his ACK packets do not contain the data needed to calculate packet success rate and he does not calculate packet success rate. As such, Chiu does not suggest modification of Jorgensen to generate IPSEC ack packets containing both sequence numbers and a value indicative of the amount of data received and to receive those IPSEC ack packets and use the aforementioned data to calculate packet success rate.

Independent Claim 13 Argument

Claim 13 contains the following limitation that distinguish it over the prior art combination applied against it:

- means for receiving acknowledgement packets for said IPSec packets,

- means for obtaining a sequence number of an IPSec packet from a received acknowledgement packet,

- means for storing in a memory means the sequence number and the transmission time of each IPSec packet transmitted by the network node via the communication link, and

- means for determining the round trip time of the communication link on the basis of the reception time of an acknowledgement packet and the stored transmission time of

the corresponding transmitted packet.

The limitations:

- means for receiving acknowledgement packets for said IPSec packets,
- means for obtaining a sequence number of an IPSec packet from a received acknowledgement packet,
- means for storing in a memory means the sequence number and the transmission time of each IPSec packet transmitted by the network node via the communication link,

should be interpreted in accordance with 35 USC 112, Para. 6 to read on the structure recited in the specification. Specifically the following portions of the specification recite the pertinent structure: page 19, lines 26-29, page 18, lines 12-15, page 21, lines 26-27, Figure 8, items 801, 870, 860, 874, 802.

The limitation:

- means for determining the round trip time of the communication link on the basis of the reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

should be interpreted in accordance with 35 USC 112, Para. 6 to read on the structure recited in the specification. Specifically, the following portions of the specification recite the pertinent structure: page 18, lines 15-18, page 21, lines 26-27.

These limitations, taken together, define a source node apparatus which receives IPSEC ack packets, each containing the sequence number of the IPSEC packet received just before the IPSEC ack packet was sent . The source node stores the transmission time of each IPSEC packet the source node sends along with its sequence number. The source node then extracts the sequence number from the received ack packet and uses that with the data stored in memory to calculate the round trip time.

Chiu is not interested in the round trip time of his reliable multicasts so Chiu does not teach storing the transmission time and sequence number of every packet transmitted and extracting the sequence numbers from the received ack packets and using the sequence numbers and the stored data to calculate the round trip time. Chiu does not have to solve the round trip time of an IPSEC tunnel to make his IPSEC multicasts reliable, so he does not suggest a solution to that particular problem to which claim 13 at bar provides a solution. The combination of Chiu and Jorgensen, even if made despite the lack of suggestion, would still fall short of the

claimed invention since the storing of transmission times in memory and the calculation of round trip times would not be present in the combination.

Independent Claims 14, 15 and 18

Claims 14, 15 and 18 all contain limitations stated in means plus function form which require means for using an IPSEC protocol communication link to tunnel IP packets between a first and second node. In addition, each of these claims contains limitations stated in means plus function format which require a means for transmitting an acknowledgment packet if at least one of a first and second conditions is fulfilled. Per the specificaton sections cited above for other claims containing similar limitations about using IPSEC tunnels and sending acknowledgment packets when either of a first or second condition is present, these limitations should be interpreted under 35 USC 112, Para. 6 to require transmission of an IPSEC acknowledgment packet to the source node in response to receipt of an IPSEC packet, said ack packet being sent when either: 1) a predetermined number of IPSEC packets has been received by the destination node; or 2) receipt of an IPSEC packet after a predetermined timeout from transmission of the last IPSEC ack packet. The ack packet is an IPSEC packet which contains at least the sequence number of the last IPSEC packet received.

Because these limitations are similar to the process limitations of claim 1 but are apparatus which perform these process steps, the argument given above for the nonobviousness of claim 1 based upon the similar process limitations is repeated here by incorporation by reference. If the prior art combination does not teach method steps to send these IPSEC ack packet or suggest sending such packets, it also does not teach a computer programmed to carry out this method.

In addition, claim 15 contains an additional limitation regarding inserting in the IPSEC ack packet a byte counter value which is indicative of the amount of data received. As noted above for other claims containing a similar process limitation, both Chiu and Jorgensen are silent on the need to include such a byte counter value in the ack packet since that value is used to calculate throughput or packet success rate, and neither end result is required in these references to solve the problems addressed by these references. The Examiner cites Col. 31, lines 50-61 of Jorgensen as teaching that the TCP protocol layer of the sender provides the TCP header for an IP packet with a byte number. This byte number is provided for purposes of reliable data flow so that the recipient can tell if all bytes have been received and send back ACK and NACK packets indicating which bytes need to be resent. In other words, the byte count of Jorgensen is

conventional TCP technology that can be used to control retransmssion of missing bytes in a packet flow. It is not intended to provide any information about the amount of data received as called for by the claims being argued here.

Accordingly, neither of these references provides a suggestion to add such a value to an IPSEC ack packet. Therefore, suggestion to combine Chiu and Jorgensen to reach the invention claimed in claim 15 is lacking, and even if the references were to be combined, the result would still fall short of claim 15 and not have the same properties or achieve the same end result.

Claim 18, properly interpreted, calls for the sending an IPSEC ack packet with the sequence number of the last received IPSEC packet in it and a value indicative of the amount of data received. In addition, it contains means plus function limitations which, properly interpreted in accordance with the specification passages recited above for similar limitations in other claims, call for apparatus to receive the IPSEC ack packets, obtain the IPSEC packet sequence numbers and values indicative of the amount of data received from the ack packet and use that extracted data to calculate the packet success rate.

Such an apparatus and method is not taught in either Chiu or Jorgensen because neither reference is addressed to the problem of measuring the performance of an IPSEC tunnel by calculating the packet success rate of transmission of transmitted IPSEC packets. Accordingly, there is no suggestion to one of skill in the art to apply the teachings of Chiu to modify the teachings of Jorgensen to extract the sequence numbers and volume of data number from the received IPSEC ack packets and calculate the packet success rate.

Independent Claims 19 and 20

Independent claims 19 and 20 are software product claims that call for media having programmed thereon instructions that control a network node to implement an IPSEC tunnel to tunnel IP packets from a source node to a destination node, and send ack packets back to the source node if either a first or second condition is fulfilled. Properly interpreted, these claims define software code containing media which controls a computer to send IPSEC ack packets under either of the two conditions recited above. These limitations are similar to the limitations discussed above for process claim 1 in the non obviousness argument, but are stated in terms of program code which controls a computer to carry out the recited process steps which are similar to the process steps recited in claim 1. As such, the nonobviousness argument given above for claim 1 is repeated here by reference.

In addition, claim 19 further defines program code means which, properly interpreted in accordance with the specification passages recited above in the section entitled SUMMARY OF

CLAIMED SUBJECT MATTER, controls a computer to receive IPSEC ack packets, extract IPSEC packet sequence numbers from them, and extract a value indicative of the amount of data received by the destination node, and calculate the packet success rate on the basis of the data extracted from the IPSEC ack packet.

Chiu is concerned with making a TCP/IP multicast reliable and teaches receiving TCP/IP ACK and NACK packets by the repair heads and then using the data in the TCP/IP ACK and NACK to resend packets in the multicast to destinations that indicated they did not receive them. No calculation of packet success rate is required for this process, and neither Chiu nor Jorgensen performs such a calculation. Accordingly, there is no suggestion to combine Chiu with Jorgensen to obtain code which controls computers to implement an IPSEC tunnel, send IPSEC ack packets which contain sequence number and volume data, receive the IPSEC ack packets and extract the sequence and volume data therefrom and calculate a packet success rate therefrom.

Claim 20 has all the limitations from claim 19 above except for extracting the volume information from the IPSEC ack packets and calculating the packet success rate. Claim 20 substitutes limitations defining computer code which controls the source node to store the sequence number and transmission time of each IPSEC packet sent in the IPSEC tunnel and receive IPSEC packets and calculate the round trip time of the IPSEC tunnel based upon reception time of the IPSEC ack packet and the stored transmission time of the IPSEC packet to which the IPSEC ack packet is a response. Since Chiu is not concerned with the round trip time of a single link in his reliable multicast protocol and he does not calculate round trip times in the multicast links, there is no suggestion to one of skill in the art to apply the teachings of Chiu to Jorgensen to arrive at code which controls a computer to use IPSEC ack packets and stored transmission times of IPSEC packets to which the IPSEC ack packets are a response to calculate round trip time of the link.

Independent Claim 9

Claim 9 and its dependent claim 10 were rejected as obvious over the combination of Jorgensen and further in view of Tam (US6,622,172) and Garcia... (US 20010013856A1). Claim 9 contains the following limitation which distinguishes it over this prior art combination:

> said method comprising at least the following steps for monitoring an active communication link between the source network site and the destination network site, the active communication link employing the IPSec protocol:
>
> the step of transmission of an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,

> said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet,

This process step of transmitting a acknowledgement packet under either of two conditions should be interpreted in the same way as the similar process step in claim 1 based upon the same intrinsic evidence recited above from the specification. The argument for nonobviousness of claim 1 is hereby incorporated by reference. The TAM teachings of sending probe packets over an inactive TCP/IP link do not alter the argument given above regarding the nonobvious of claim 1 and other claims which contain a limitation like that cited above. The teachings of Garcia of measuring link delays and replacing active links with inactive links based upon the result of monitoring, do not alter the argument given above regarding the nonobvious of claim 1 and other claims which contain a limitation like that cited above.

Accordingly, the prior art combination still teaches away from sending IPSEC ack packets which contain IPSEC packet sequence numbers under one of two conditions, and the prior art combination of Jorgensen and Chiu would be inoperative and not have the desired properties needed to make the invention. The prior art combination of Jorgensen and Chiu is still lacking the knowledge needed to make the invention including the limitation recited above. Tam teaches probing a TCP protocol communication link but does not teach monitoring an inactive IPSEC link between a source node and a destination node which has an active IPSEC link which is monitored at the same time. Further, neither Chiu nor Tam teach maintaining the present status of the active and inactive IPSEC links or replacing the active link with an inactive link based upon the results of the monitoring. Finally, neither Chiu nor Tam teach calculating the roundtrip time of the inactive link. All this is what claim 9 calls for.

Therefore, there is no suggestion to combine Chiu with Jorgensen to achieve the limitation recited above. The addition of Tam and Garcia to this prior art combination does not change this conclusion. This is because neither of these prior art references teaches generation of IPSEC ack packets with sequence number of the IPSEC packet just received in an IPSEC tunnel, said ack packet being sent if either one of two conditions are met. Accordingly claim 9 is not obvious for lack of suggestion to make the proposed combination. Since claim 9 is not obvious, its more narrow dependent claim is also not obvious.

CLAIMS APPENDIX

1. [currently amended] Method for monitoring of a communication link between a source network node and a destination network node, comprising

- employing, on said communication link, the IPSec protocol for tunneling P packets between the source network node and the destination network node,

- transmitting an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled, said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and said second condition being the reception of an IPSec packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

2. [currently amended] Method for monitoring of a communication link between a source network node and a destination network node, comprising

- employing, on said communication link, the IPSec protocol for tunneling P packets between the source network node and the destination network node,

- transmitting an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,, wherein said acknowledgement packet comprises at least the sequence number of the last received IPSec packet and at least one value corresponding to the amount of data received via the IPSec communication link,

said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and

said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet..

3. [original] A method according to claim 2, wherein said acknowledgement packet comprises at least a packet counter value indicating the number of packets received via the communication link.

4. [original] A method according to claim 2, wherein said acknowledgement packet comprises at least a byte counter value indicating the number of bytes received via the communication link.

5. [original] A method according to claim 2, wherein said acknowledgement packet comprises at least a packet counter value indicating the number of packets received via the communication link and a byte counter value indicating the number of bytes received via the communication link.

6. [original] A method according to claim 2, further comprising at least the step of determining the packet success rate of the communication link at least partly on the basis of information contained in an acknowledgement packet.

7. [original] A method according to claim 2, further comprising at least the step of determining the throughput of the communication link at least partly on the basis of information contained in an acknowledgement packet.

8. [currently amended] A method for monitoring of a communication link between a source network node and a destination network node, comprising

- employing, on said communication link, the IPSec protocol for tunneling IP packets between the source network node and the destination network node,
- transmitting an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,

said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and

said second condition being the reception of an IPSec packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet

- storing of the sequence number and the transmission time of each IPSec packet transmitted from the source network node to the destination network node in a memory means, and
- determining the round trip time of the communication link on the basis of the

reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

9. [currently amended] Method for monitoring of a plurality of communication links between a source network site and a destination network site, each of the sites having at least one network node,
in which method an active communication link is monitored and an inactive communication link is monitored,
said method comprising at least the following steps for monitoring an active communication link between the source network site and the destination network site, the active communication link employing the IPSec protocol:

the step of transmission of an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,

said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and

said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet,

and said method comprising at least the following steps for monitoring an inactive communication link between the source network site and the destination network site:

- transmitting a probe packet from a source node at the source network site via said inactive communication link to a destination node at the destination network site,
- storing the transmission time of said probe packet in a memory means,
- transmitting a response packet from said destination node to said source node as a response to receiving a probe packet,
- determining the round trip time of said inactive communication link from the difference of the reception time of the response packet and the stored transmission time of the corresponding probe packet
- maintaining present status of said active and inactive communications links or replacing said active communication link with said inactive communication link based on results of said monitoring.

10. [original] A method according to claim 9, said method further comprising the steps of
- transmitting a plurality of probe packets from said source node at the source network site via said inactive communication link to said destination node at the destination network site,
- receiving response packets to said probe packets, and
- determining the packet success rate of said inactive communication link from the number of said received response packets and the number of transmitted probe packets.

11. [currently amended] A network node comprising at least
- means for communicating over a IPSec protocol communication link with a second network node using IPSec packets in order to tunnel IP packets transmitted to said second network node,
- means for sending acknowledgment packets for said IPSec packets containing IP packets,
- means for receiving said acknowledgement packets for said IPSec packets,
- means for obtaining a sequence number of an IPSec packet from said a received acknowledgement packet,
- means for obtaining a value from said the acknowledgement packet, said value corresponding to the amount of data received via the communication link by said second network node, and
- means for determining the packet success rate of the communication link at least partly on the basis of said value.

12. [original] A network node according to claim 11, further comprising at least means for determining the throughput of the communication link at least partly on the basis of said value.

13. [currently amended] A network node comprising at least
- means for communicating over a IPSec protocol communication link with a second network node in order to tunnel IP packets transmitted to said second network node,
- means for sending IPSec packets containing IP packets,

- means for receiving acknowledgement packets for said IPSec packets,
- means for obtaining a sequence number of an IPSec packet from a received acknowledgement packet,
- means for storing in a memory means the sequence number and the transmission time of each IPSec packet transmitted by the network node via the communication link, and
- means for determining the round trip time of the communication link on the basis of the reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

14. [currently amended] A network node for communicating with the IPSec protocol with a second network node via a communication link, said network node comprising at least
- means for communicating over a IPSec protocol communication link with a second network node in order to tunnel IP packets transmitted from said second network node,
- means for sending IPSec packets containing IP packets,
- means for transmission of transmitting an acknowledgement packet if at least one of a first condition and a second condition is fulfilled,
said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and
said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

15. [currently amended] A network node comprising at least
- means for communicating over a IPSec protocol communication link with a second network node in order to tunnel IP packets transmitted from said second network node,
- means receiving IPSec packets containing IP packets,
- means transmitting an acknowledgement packet if at least one of a first condition and a second condition is fulfilled,-
- means for inserting a sequence number of a received IPSec packet and at

least one value corresponding to the amount of data received via the communication link in said acknowledgement packet,

said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and

said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

16. [currently amended] A network node according to claim 15, said network node further comprising at least means for inserting a packet counter value in said acknowledgement packet, said packet counter value indicating the number of packets received via the communication link.

17. [currently amended] A network node according to claim 15, said network node further comprising at least means for inserting a byte counter value in said acknowledgement packet, said byte counter value indicating the number of bytes received via the communication link.

18. [currently amended] A network node comprising at least

- means for communicating over a IPSec protocol communication link with a second network node in order to tunnel IP packets transmitted from said second network node,

- means for transmitting an acknowledgement packet if at least one of a first condition and a second condition is fulfilled,

said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and

said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet,

- means for sending IPSec packets,

- means for receiving acknowledgement packets for said IPSec packets transmitted by the network node,

- means for obtaining a sequence number of an IPSec packet from a received

acknowledgement packet,

- means for obtaining a value from the acknowledgement packet, said value corresponding to the amount of data received via the communication link by the second network node, and

- means for determining the packet success rate of the communication link at least partly on the basis of said value.

19. [currently amended] Software program product for a network node for communicating with the IPSec protocol with a second network node via a communication link, said software program product comprising at least

- software program code communicating over a IPSec protocol communication link with a second network node in order to tunnel IP packets transmitted from said second network node,

- software program code receiving IPSec packets containing IP packets,

- software program code means for transmission of transmitting an acknowledgement packet if at least one of a first condition and a second condition is fulfilled,

said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and

said second condition being the reception of a packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet,

- software program code means for receiving acknowledgement packets for IPSec packets transmitted by the network node,

- software program code means for obtaining a sequence number of an IPSec packet from a received acknowledgement packet,

- software program code means for obtaining a value from the acknowledgement packet, said value corresponding to the amount of data received via the communication link by the second network node, and

- software program code means for determining the packet success rate of the communication link at least partly on the basis of said value.

20. [new] Software program product for a network node for communicating with the IPSec protocol with a second network node via a communication link, said software program product comprising at least

- software program code communicating over a IPSec protocol communication link with a second network node in order to tunnel IP packets transmitted to said second network node,
- software program code sending IPSec packets containing IP packets,
- software program code receiving acknowledgement packets for said IPSec packets,
- software program code obtaining a sequence number of an IPSec packet from a received acknowledgement packet,
- software program code storing in a memory means the sequence number and the transmission time of each IPSec packet transmitted by the network node via the communication link, and
- software program code determining the round trip time of the communication link on the basis of the reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

21. [new] Method for monitoring of a communication link between a source network node and a destination network node, comprising

- employing, on said communication link, the IPSec protocol for tunneling IP packets of one or more TCP/IP connections between the source network node and the destination network node,
- transmitting, separately from TCP retransmission scheme carried out on said one or more TCP/IP connections, an acknowledgement packet by the destination network node if at least one of a first condition and a second condition is fulfilled,
  - said first condition being the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgement packet, and
  - said second condition being the reception of an IPSec packet via the communication link after a predetermined time has passed after transmission of the previous acknowledgement packet.

22. [new] A method according to claim 21, comprising tunneling IP packets of two or more TCP/IP connections by means of said communication link using the IPSec protocol.

EVIDENCEAPPENDIX

None

RELATEDPROCEEDINGSAPPENDIX

None

Respectfully Submitted

Ronald C. Fish

Ronald Craig Fish
Reg. No. 28,843
Tel 408 866 4777
Attorney for Applicant(s)

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on 5/20/05
(Date of Deposit)

Ronald C. Fish

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843